Network Planning Guide for ProSafe VPN Firewall Router FVX538

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10066-01 (Beta Draft)
October 2004

© 2004 by NETGEAR, Inc. All rights reserved. FullManual.

Trademarks

NETGEAR and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc..

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

October 2004

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Export Restrictions

The NETGEAR VPN Client (the “software”) is subject to United States Export Controls. The software may not be exported or transmitted 1) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Syria, Sudan or any other country to which the United States has embargoed goods; or 2) to anyone on the United States Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders. By using this software, you agree to abide by the laws, rules and regulations - including, but not limited to the Export Administration Act and the Arms Export Control Act - applicable to such use and not to transfer, by electronic transmission or otherwise, the software to either a foreign national or a foreign destination in violation of any such laws.

Contents

Chapter 1
Introducing the FVX538

The Router's Front Panel 1-1
The Router's Rear Panel 1-3
Rack Mounting the Router 1-3
The Router's IP Address, Login Name, and Password 1-4
Default Factory Settings 1-4

Chapter 2
Network Planning

Overview of the Planning Process 2-1
Single or Multiple Exposed Hosts 2-1
Virtual Private Networks (VPNs) 2-2
The Fail-over Case for Routers With Dual WAN Ports 2-2
The Load Balancing Case for Routers With Dual WAN Ports 2-2
Single or Multiple Exposed Hosts 2-3
Single Exposed Host 2-3
Multiple Exposed Hosts 2-5
Virtual Private Networks (VPNs) 2-6
VPN Road Warrior (Client-to-Gateway) 2-8
VPN Gateway-to-Gateway 2-10
VPN Telecommuter (Client-to-Gateway Through a NAT Router) 2-13

Chapter 1
Introducing the FVX538

This chapter introduces the FVX538 ProSafe VPN Firewall Router.

The Router's Front Panel

The FVX538 ProSafe VPN Firewall Router front panel shown below contains the port connections, status LEDs, and the factory defaults reset button.

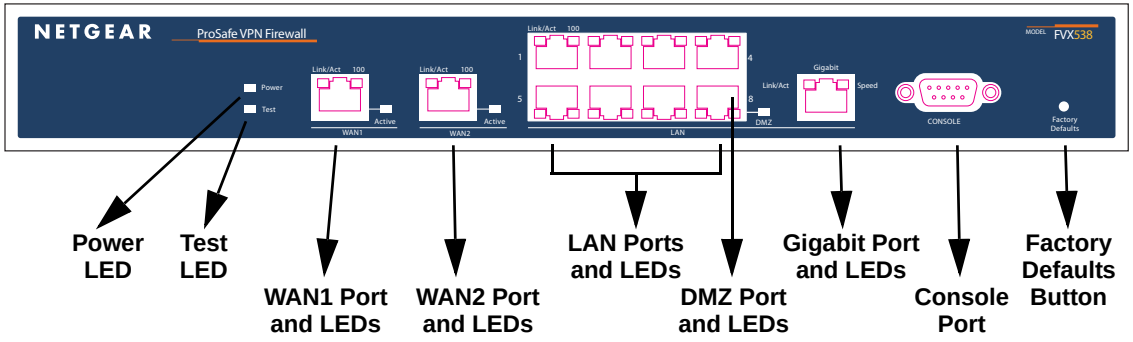

Figure 1-1: FVX538 Front Panel

You can use the LEDs to verify various conditions. Table 1-1 lists and describes each object on the front panel of the router and its operation.

Table 1-1. Object Descriptions

Object	Activity	Description
Power LED	On (Green) Off	Power is supplied to the router. Power is not supplied to the router.
Test LED	On (Amber) Blinking (Amber) Off	Test mode: The system is initializing or the initialization has failed. Writing to Flash memory (during upgrading or resetting to defaults). The system has booted successfully.

Table 1-1. Object Descriptions (continued)

Object	Activity	Description
WAN Ports and LEDs	Two RJ-45 WAN ports	N-way automatic speed negotiation, Auto MDI/MDIX.
	Link/Act LED On (Green) Blinking (Green) Off	 The WAN port has detected a link with a connected Ethernet device. Data is being transmitted or received by the WAN port. The WAN port has no link.
	100 LED On (Green) Off	 The WAN port is operating at 100 Mbps. The WAN port is operating at 10 Mbps.
	Active LED On (Green) On (Amber) Off	 The WAN port has a valid Internet connection. The Internet connection is down. The WAN port is either not enabled or has no link.
LAN Ports and LEDs	8-port RJ-45 10/100 Mbps Fast Ethernet Switch	N-way automatic speed negotiation, auto MDI/MDIX.
	Link/Act LED On (Green) Blinking (Green) Off	 The LAN port has detected a link with a connected Ethernet device. Data is being transmitted or received by the LAN port. The LAN port has no link.
	100 LED On (Green) Off	 The LAN port is operating at 100 Mbps. The LAN port is operating at 10 Mbps.
	DMZ (port 8) On (Green) Off	 Port 8 is operating as a dedicated hardware DMZ port. Port 8 is operating as a normal LAN port.
Gigabit Port and LEDs	Gbit RJ-45 connector	Port for connecting to a gigabit Ethernet device.
	Link/Act LED On (Green) Blinking (Green) Off	 The LAN port has detected a link with a connected Ethernet device. Data is being transmitted or received by the LAN port. The LAN port has no link.
	Speed LED On (Green) On (Amber) Off	 The LAN port is operating at 1,000 Mbps. The LAN port is operating at 100 Mbps. The LAN port is operating at 10 Mbps.
Console Port	DB9 male connector	Port for connecting to an optional console terminal. Default baud rate is 9,600; pinouts: (2) Tx, (3) Rx, (5) and (7) Gnd.
Factory Defaults	—	Factory Defaults reset push button (see “Default Factory Settings” on page 1-4 for the factory defaults).

The Router's Rear Panel

The rear panel of the FVX538 ProSafe VPN Firewall Router (Figure 1-2) contains the On/Off switch and AC power connection.

Figure 1-2: FVX538 Rear Panel

Viewed from left to right, the rear panel contains the following elements:

- AC power in
- On/Off switch

Rack Mounting the Router

The FVX538 can be mounted either on a desktop (using included rubber feet) or in a 19-inch rack (using the included rack mounting hardware illustrated in Figure 1-3).

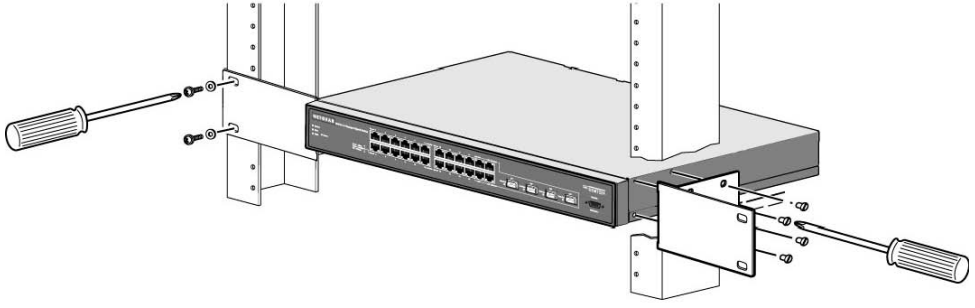

Figure 1-3: Attaching Mounting Brackets

The Router's IP Address, Login Name, and Password

Check the label on the bottom of the FVX538's enclosure if you forget the following factory default information:

- IP Address: **http://192.168.1.1** to reach the Web-based GUI from the LAN
- User name: **admin**
- Password: **password**

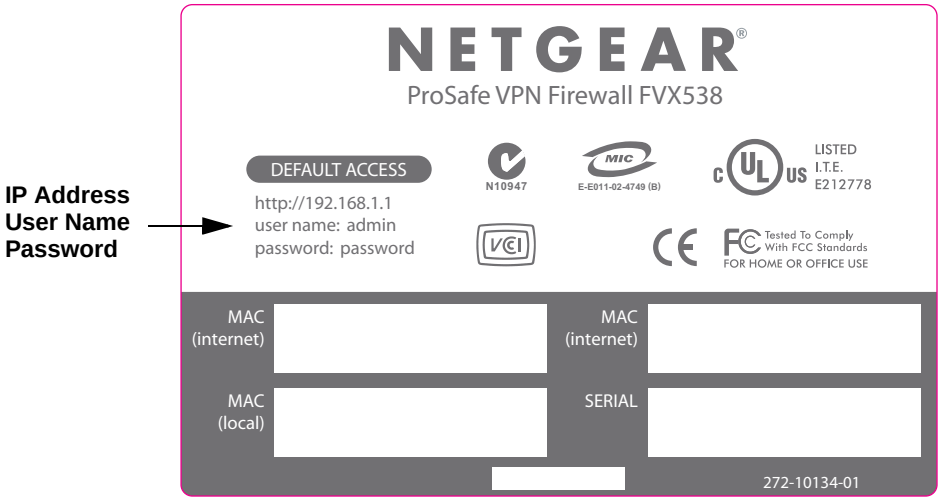

Figure 1-4: FVX538 Bottom Label

Default Factory Settings

When you first receive your FVX538, the default factory settings will be set as shown in Table 1-2 below. You can restore these defaults with the Factory Defaults restore switch on the front panel — see "The Router's Front Panel" on page 1-1.

- Pressing this switch for a prolonged period (>5 seconds) causes the router to restore all factory default settings and reboot.
- A shorter press and release causes the router to merely reboot.

Table 1-2. Factory Default Settings

Feature	Default
User Name (case sensitive)	**admin**
Password (case sensitive)	**password**
Built-in DHCP server	**DHCP server is enabled, issues addresses in the default subnet**
IP Configuration	**IP Address: 192.168.1.1** **Subnet Mask: 255.255.255.0** **Gateway: 0.0.0.0**
Time Zone	**GMT**
Time Zone Adjust for Daylight Saving TIme	**Disabled**
SNMP	**Disabled**

Chapter 2
Network Planning

This chapter describes the factors to consider when planning a network using a router that has dual WAN ports.

Overview of the Planning Process

The areas that require planning when using a router that has dual WAN ports include:

- Single or multiple exposed hosts
- Virtual private networks (VPNs)

Note: Exposed hosts are sometimes referred to as DMZ hosts. Unlike hardware-based DMZ ports, however, exposed hosts are implemented in software and do not enjoy the same level of firewall protection that hardware-based DMZ ports do. Use the exposed host feature at your own risk.

The two WAN ports can be configured on a mutually-exclusive basis to either:

- Fail over for increased system reliability, or
- Balance the load for outgoing traffic

These two categories of considerations interact to make the planning process more challenging.

Single or Multiple Exposed Hosts

Unrequested incoming traffic can be directed to one or more exposed hosts rather than being discarded. As a result, the IP address of at least one WAN port must always be public.

The mechanism for making the IP address public depends on whether there are single or multiple exposed hosts and whether the dual WAN ports are configured to either fail over or balance the loads. See “Single or Multiple Exposed Hosts” on page 2-3 for further discussion.

Virtual Private Networks (VPNs)

A virtual private network (VPN) tunnel provides a secure communication channel between either two gateway VPN routers or between a remote PC client and gateway VPN router. As a result, the IP address of at least one of the tunnel end points must be known in advance in order for the other tunnel end point to establish (or re-establish) the VPN tunnel. See "Virtual Private Networks (VPNs)" on page 2-6 for further discussion.

Note: Once the gateway router WAN port fails over, the VPN tunnel collapses and must be re-established using the new WAN IP address.

The Fail-over Case for Routers With Dual WAN Ports

Failover (Figure 2-1) for the dual WAN port case is different from the single gateway WAN port case when specifying the IP address. Only one WAN port is active at a time and when it fails over, the IP address of the active WAN port always changes. Hence, the use of a fully-qualified domain name is always required, even when the IP address of each WAN port is fixed.

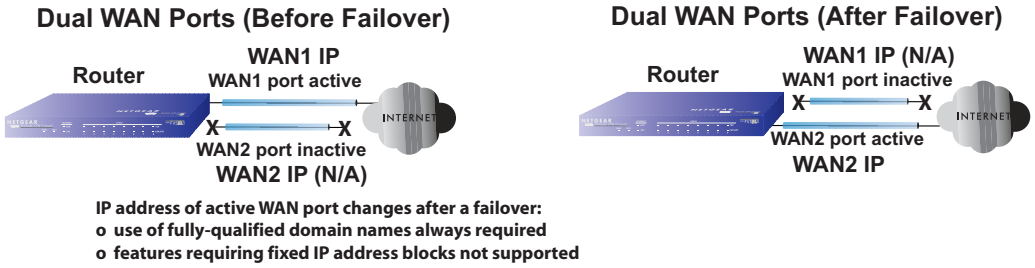

Figure 2-1: Dual WAN ports before and after failover

Features such as multiple exposed hosts are not supported when using dual WAN port failover because the IP addresses of each WAN port must be in the identical range of fixed addresses.

The Load Balancing Case for Routers With Dual WAN Ports

Load balancing (Figure 2-2) for the dual WAN port case is similar to the single WAN port case when specifying the IP address. Each IP address is either fixed or dynamic based on the ISP: fully-qualified domain names must be used when the IP address is dynamic and are optional when the IP address is static.

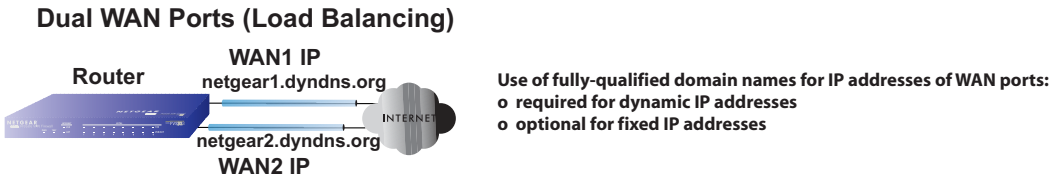

Figure 2-2: Dual WAN ports for load balancing

Single or Multiple Exposed Hosts

Incoming traffic from the Internet is normally discarded by the firewall unless the traffic is a response to one of your local computers or a service that you have configured in the Inbound Rules menu. Instead of discarding this traffic, you can have it forwarded to one or more LAN hosts on your network. These LAN hosts are called exposed hosts.

The addressing of the router's dual WAN port depends on the configuration being implemented:

Table 2-1. IP addressing requirements for exposed hosts in dual WAN port systems

Configuration and WAN IP address		Single WAN Port (reference case)	Dual WAN Port Cases	
			Failover	Load Balancing
Single exposed host	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required
Multiple exposed hosts	Fixed	Address block required (FQDN optional)	Not allowed[a]	Address block required (FQDN optional)
	Dynamic	Not allowed	Not allowed	Not allowed

a. Not allowed because to do so, the IP addresses of each WAN port would have to be the identical range of fixed addresses.

Single Exposed Host

The Internet IP address of the router's WAN port must be known to the public so that the public can send incoming traffic to the exposed host when this feature is supported and enabled.

Single Exposed Host: Single WAN Port (Reference Case)

In the single WAN case (Figure 2-3), the WAN's Internet address is either fixed IP or a fully-qualified domain name if the IP address is dynamic.

Figure 2-3: Single WAN port case with exposed host

Single Exposed Host: Dual WAN Ports for Improved System Reliability

In the dual WAN port case with failover (Figure 2-4), the WAN's IP address will always change at failover. A fully-qualified domain name must be used that toggles between the IP addresses of the WAN ports (i.e., WAN1 or WAN2).

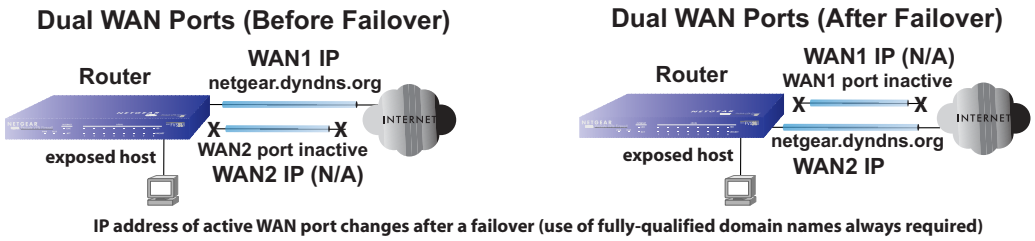

Figure 2-4: Dual WAN port case with exposed host, before and after failover

Single Exposed Host: Dual WAN Ports for Load Balancing

In the dual WAN port case for load balancing (Figure 2-5), the Internet address of each WAN port is either fixed if the IP address is fixed or a fully-qualified domain name if the IP address is dynamic.

	Note: Load balancing is implemented for outgoing traffic and not for incoming traffic. Consider making one of the WAN port Internet addresses public and keeping the other one private in order to maintain better control of WAN port traffic.

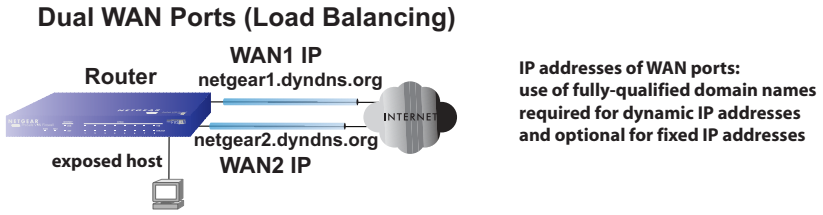

Figure 2-5: Dual WAN port case for exposed host with load balancing

Multiple Exposed Hosts

The IP address range of the router's WAN port must be both fixed and public so that the public can send incoming traffic to the multiple exposed hosts when this feature is supported and enabled.

Multiple Exposed Hosts: Single WAN Port (Reference Case)

In the single WAN case (Figure 2-6), the WAN port's IP address range must be fixed.

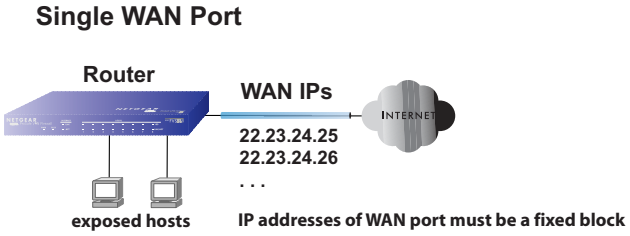

Figure 2-6: Single WAN port case with multiple exposed hosts

Multiple Exposed Hosts: Dual WAN Ports for Improved System Reliability

Using multiple exposed hosts with routers that have dual WAN ports for improved system reliability is a disallowed combination because to do so, the IP addresses of each WAN port would have to be the identical range of fixed addresses. Instead, use additional routers that have dual WAN ports with a single exposed host for improved system reliability.

Multiple Exposed Hosts: Dual WAN Ports for Load Balancing

In the dual WAN port case for load balancing (Figure 2-7), the IP address range of each WAN port must be fixed.

Note: Load balancing is implemented for outgoing traffic and not for incoming traffic. Consider publicizing one of the WAN port Internet addresses and keeping the other one unpublicized in order to maintain better control of WAN port traffic.

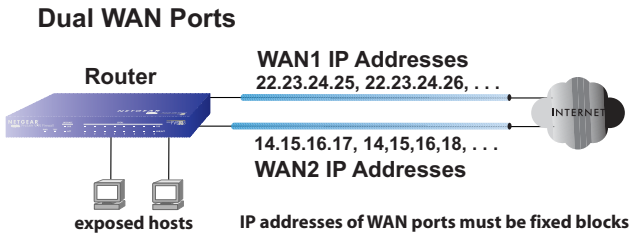

Figure 2-7: Dual WAN port case for multiple exposed hosts with load balancing

Virtual Private Networks (VPNs)

When implementing virtual private network (VPN) tunnels, a mechanism must be used for determining the IP addresses of the tunnel end points. The addressing of the router's dual WAN port depends on the configuration being implemented:

Table 2-1. IP addressing requirements for VPNs in dual WAN port systems

Configuration and WAM IP address		Single WAN Port (reference case)	Dual WAN Port Cases	
			Failover[a]	Load Balancing
VPN Road Warrior (client-to-gateway)	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required
VPN Gateway-to-Gateway	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required
VPN Telecommuter (client-to-gateway through a NAT router)	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required

a. All tunnels must be re-established after a failover using the new WAN IP adress.

For the single gateway WAN port case, the mechanism is to use a fully-qualified domain name (FQDN) when the IP address is dynamic and to use either an FQDN or the IP address itself when the IP address is fixed. The situation is different when dual gateway WAN ports are used in a failover-based system.

- Failover Case for Dual Gateway WAN Ports

  Failover (Figure 2-8) for the dual gateway WAN port case is different from the single gateway WAN port case when specifying the IP address of the VPN tunnel end point. Only one WAN port is active at a time and when it fails over, the IP address of the active WAN port always changes. Hence, the use of a fully-qualified domain name is always required, even when the IP address of each WAN port is fixed.

Note: Once the gateway router WAN port fails over, the VPN tunnel collapses and must be re-established using the new WAN IP address.

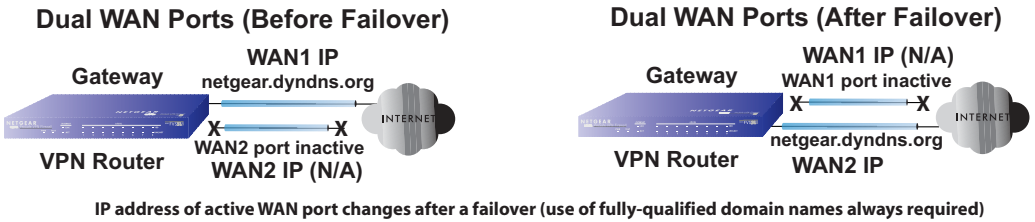

Figure 2-8: Dual gateway WAN ports before and after failover

- Load Balancing Case for Dual Gateway WAN Ports

  Load balancing (Figure 2-9) for the dual gateway WAN port case is the same as the single gateway WAN port case when specifying the IP address of the VPN tunnel end point. Each IP address is either fixed or dynamic based on the ISP: fully-qualified domain names must be used when the IP address is dynamic and are optional when the IP address is static.

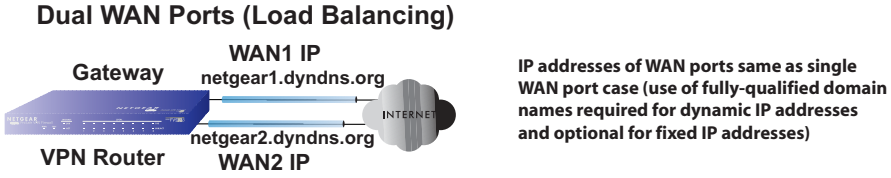
Dual WAN Ports (Load Balancing)
Gateway
WAN1 IP
netgear1.dyndns.org
INTERNET
netgear2.dyndns.org
VPN Router
WAN2 IP
IP addresses of WAN ports same as single WAN port case (use of fully-qualified domain names required for dynamic IP addresses and optional for fixed IP addresses)

Figure 2-9: Dual gateway WAN ports for load balancing

VPN Road Warrior (Client-to-Gateway)

The following situations exemplify the requirements for a remote PC client with no router to establish a VPN tunnel with a gateway VPN router:

- Single gateway WAN port
- Redundant dual gateway WAN ports for increased system reliability (before and after failover)
- Dual gateway WAN ports used for load balancing

VPN Road Warrior: Single Gateway WAN Port (Reference Case)

In the case of the single WAN port on the gateway VPN router (Figure 2-10), the remote PC client initiates the VPN tunnel because the IP address of the remote PC client is not known in advance. The gateway WAN port must act as the responder.

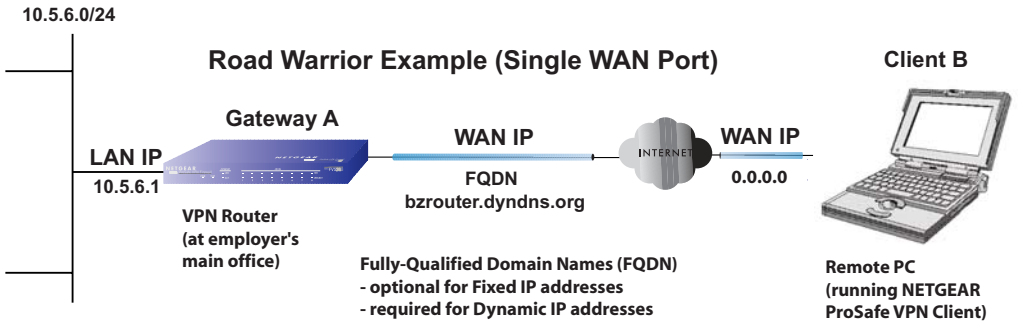

Figure 2-10: Single gateway WAN port case for VPN road warrior

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, a fully-qualified domain name must be used. If the IP address is fixed, a fully-qualified domain name is optional.

VPN Road Warrior: Dual Gateway WAN Ports for Improved System Reliability

In the case of the dual WAN ports on the gateway VPN router (Figure 2-11), the remote PC client initiates the VPN tunnel with the active gateway WAN port (port WAN1 in this example) because the IP address of the remote PC client is not known in advance. The gateway WAN port must act as a responder.

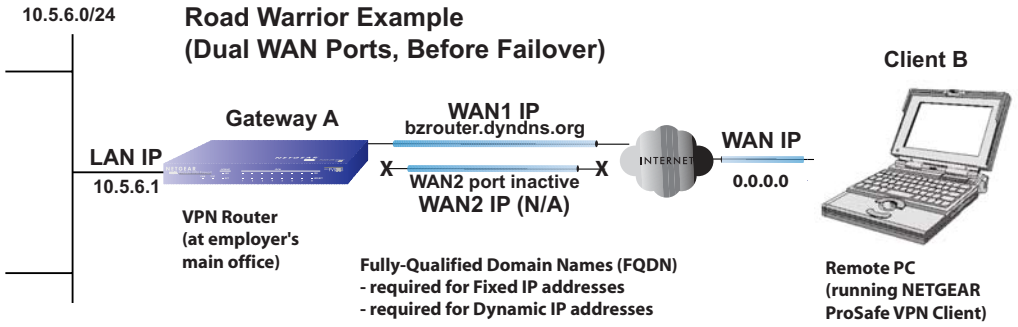

Figure 2-11: Dual gateway WAN ports, before failover, for VPN road warrior

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but a fully-qualified domain name must always be used because the active WAN port could be either WAN1 or WAN2 (i.e., the IP address of the active WAN port is not known in advance).

After a failover of the gateway WAN port (Figure 2-12), the previously inactive gateway WAN port becomes the active port (port WAN2 in this example) and the remote PC client must re-establish the VPN tunnel. The gateway WAN port must act as the responder.

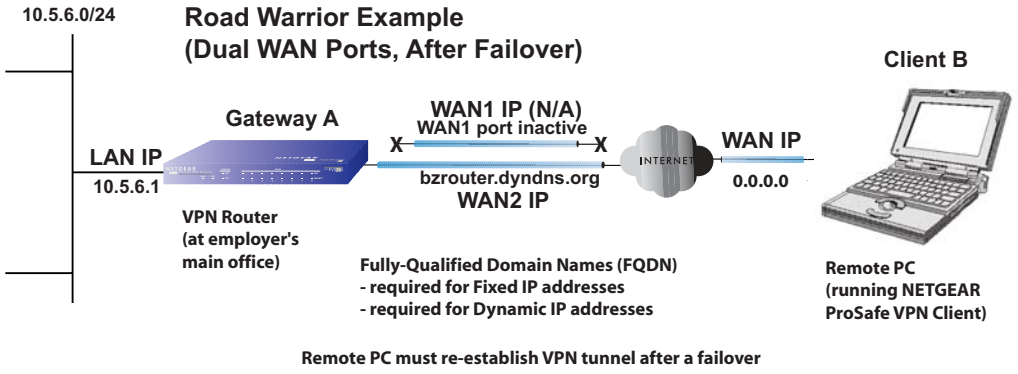

Figure 2-12: Dual gateway WAN ports, after failover, for VPN road warrior

The purpose of the fully-qualified domain name is this case is to toggle the domain name of the gateway router between the IP addresses of the active WAN port (i.e., WAN1 and WAN2) so that the remote PC client can determine the gateway IP address to establish or re-establish a VPN tunnel.

VPN Road Warrior: Dual Gateway WAN Ports for Load Balancing

In the case of the dual WAN ports on the gateway VPN router (Figure 2-13), the remote PC initiates the VPN tunnel with the appropriate gateway WAN port (i.e., port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the remote PC is not known in advance. The chosen gateway WAN port must act as the responder.

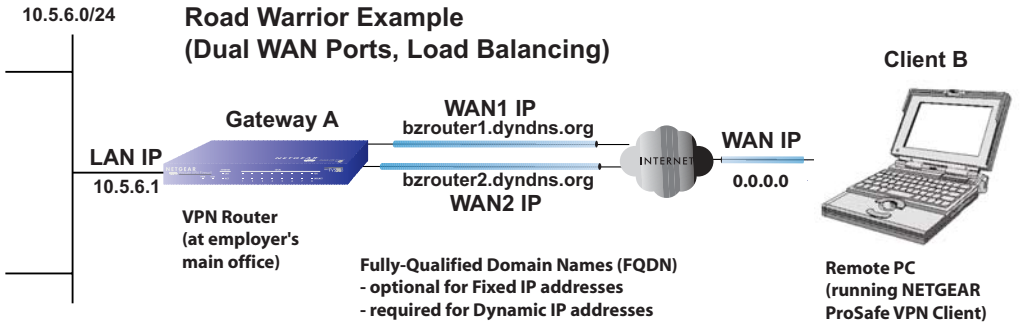

Figure 2-13: Dual gateway WAN ports (load balancing case) for VPN road warrior

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, a fully-qualified domain name must be used. If an IP address is fixed, a fully-qualified domain name is optional.

VPN Gateway-to-Gateway

The following situations exemplify the requirements for a gateway VPN router to establish a VPN tunnel with another gateway VPN router:

- Single gateway WAN ports
- Redundant dual gateway WAN ports for increased system reliability (before and after failover)
- Dual gateway WAN ports used for load balancing

VPN Gateway-to-Gateway: Single Gateway WAN Ports (Reference Case)

In the case of single WAN ports on the gateway VPN routers (Figure 2-14), either gateway WAN port can initiate the VPN tunnel with the other gateway WAN port because the IP addresses are known in advance.

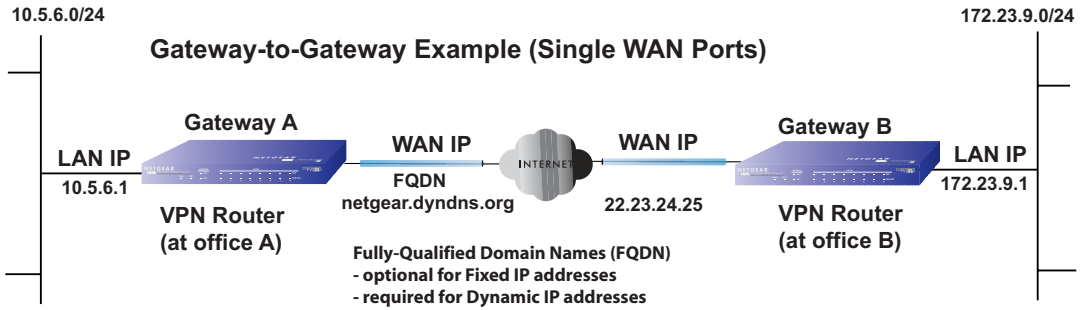

Figure 2-14: Single gateway WAN ports case for gateway-to-gateway VPN tunnels

The IP address of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, a fully-qualified domain name must be used. If an IP address is fixed, a fully-qualified domain name is optional.

VPN Gateway-to-Gateway: Dual Gateway WAN Ports for Improved System Reliability

In the case of the dual WAN ports on the gateway VPN router (Figure 2-15), either of the gateway WAN ports at one end can initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to balance the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance. In this example, port WAN_A1 is active and port WAN_A2 is inactive at Gateway A; port WAN_B1 is active and port WAN_B2 is inactive at Gateway B.

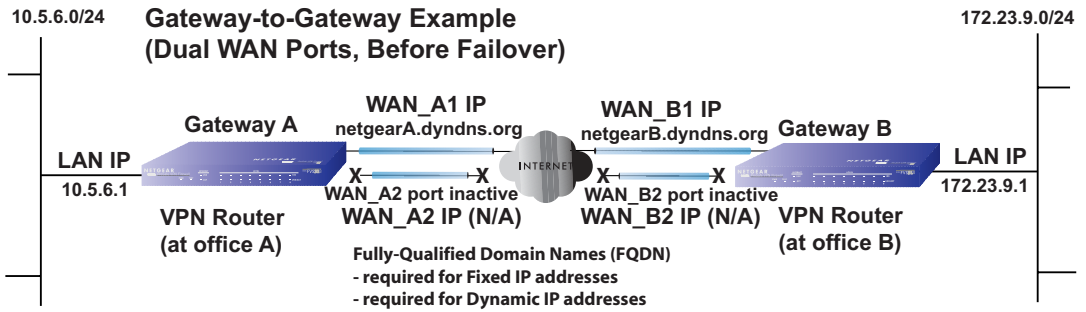

Figure 2-15: Dual gateway WAN ports, before failover, for gateway-to-gateway VPN tunnels

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but a fully-qualified domain name must always be used because the active WAN ports could be either WAN_A1, WAN_A2, WAN_B1, or WAN_B2 (i.e., the IP address of the active WAN port is not known in advance).

After a failover of a gateway WAN port (Figure 2-16), the previously inactive gateway WAN port becomes the active port (port WAN_A2 in this example) and one of the gateway VPN routers must re-establish the VPN tunnel.

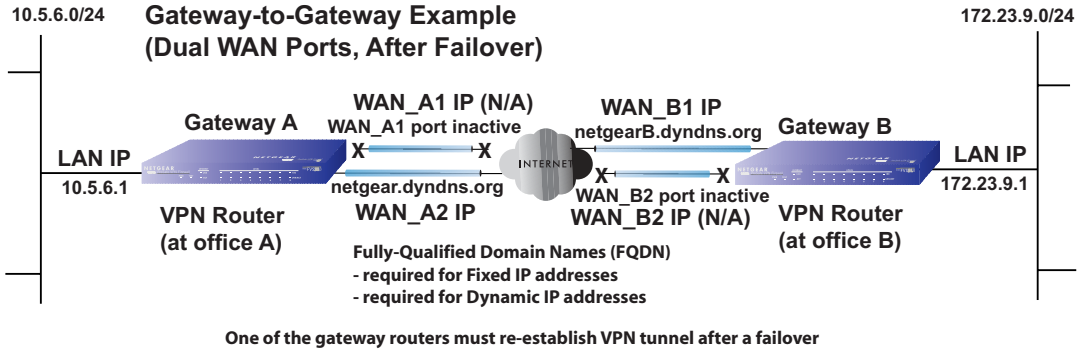

Figure 2-16: Dual gateway WAN ports, after failover, for gateway-to-gateway VPN tunnels

The purpose of the fully-qualified domain names is this case is to toggle the domain name of the failed-over gateway router between the IP addresses of the active WAN port (i.e., WAN_A1 and WAN _A2 in this example) so that the other end of the tunnel has a known gateway IP address to establish or re-establish a VPN tunnel.

VPN Gateway-to-Gateway: Dual Gateway WAN Ports for Load Balancing

In the case of the dual WAN ports on the gateway VPN router (Figure 2-17), either of the gateway WAN ports at one end can be programmed in advance to initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to manage the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance.

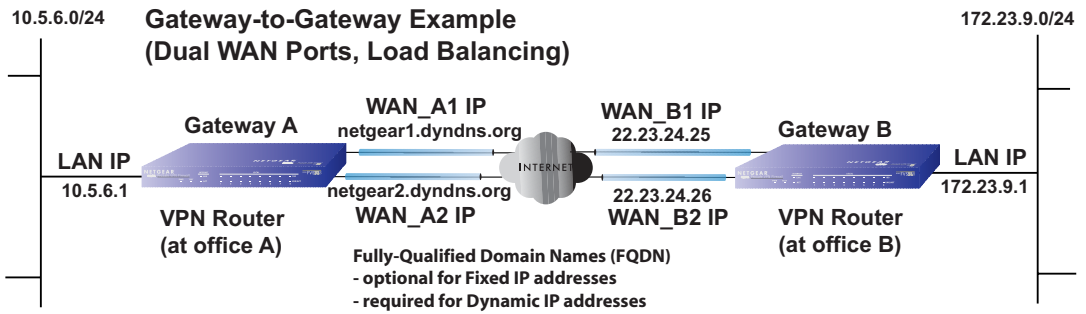

Figure 2-17: Dual gateway WAN ports (load balancing case) for gateway-to-gateway VPN tunnels

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, a fully-qualified domain name must be used. If an IP address is fixed, a fully-qualified domain name is optional.

VPN Telecommuter (Client-to-Gateway Through a NAT Router)

Note: The telecommuter case presumes the home office has a dynamic IP address and NAT router for budgetary reasons.

The following situations exemplify the requirements for a remote PC client connected to the Internet with a dynamic IP address through a NAT router to establish a VPN tunnel with a gateway VPN router at the company office:

- Single gateway WAN port
- Redundant dual gateway WAN ports for increased system reliability (before and after failover)
- Dual gateway WAN ports used for load balancing

VPN Telecommuter: Single Gateway WAN Port (Reference Case)

In the case of the single WAN port on the gateway VPN router (Figure 2-18), the remote PC client at the NAT router initiates the VPN tunnel because the IP address of the remote NAT router is not known in advance. The gateway WAN port must act as the responder.

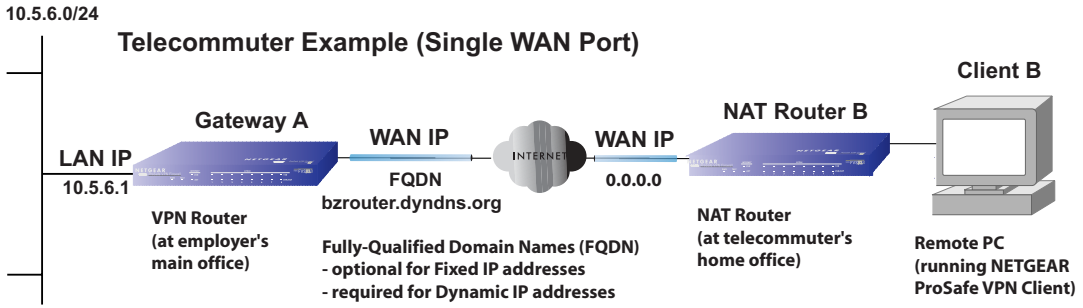

Figure 2-18: Single gateway WAN port case for VPN telecommuter

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, a fully-qualified domain name must be used. If the IP address is fixed, a fully-qualified domain name is optional.

VPN Telecommuter: Dual Gateway WAN Ports for Improved System Reliability

In the case of the dual WAN ports on the gateway VPN router (Figure 2-19), the remote PC client initiates the VPN tunnel with the active gateway WAN port (port WAN1 in this example) because the IP address of the remote NAT router is not known in advance. The gateway WAN port must act as the responder.

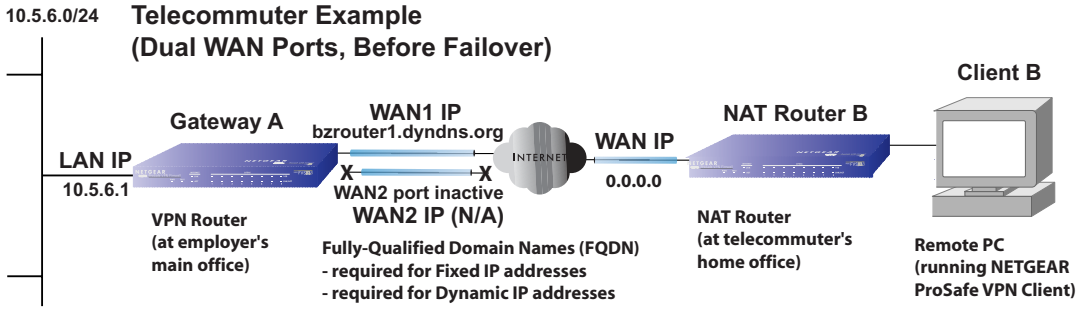

Figure 2-19: Dual gateway WAN ports, before failover, for VPN telecommuter

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but a fully-qualified domain name must always be used because the active WAN port could be either WAN1 or WAN2 (i.e., the IP address of the active WAN port is not known in advance).

After a failover of the gateway WAN port (Figure 2-20), the previously inactive gateway WAN port becomes the active port (port WAN2 in this example) and the remote PC must re-establish the VPN tunnel. The gateway WAN port must act as the responder.

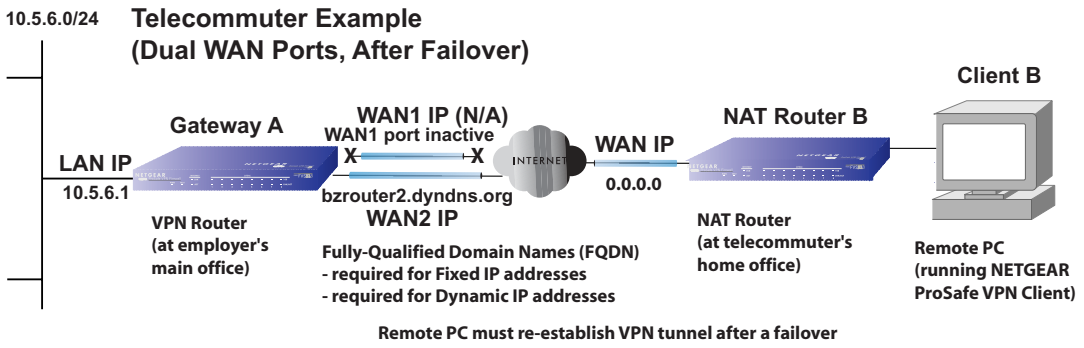

Figure 2-20: Dual gateway WAN ports, after failover, for VPN telecommuter

The purpose of the fully-qualified domain name is this case is to toggle the domain name of the gateway router between the IP addresses of the active WAN port (i.e., WAN1 and WAN2) so that the remote PC client can determine the gateway IP address to establish or re-establish a VPN tunnel.

VPN Telecommuter: Dual Gateway WAN Ports for Load Balancing

In the case of the dual WAN ports on the gateway VPN router (Figure 2-21), the remote PC client initiates the VPN tunnel with the appropriate gateway WAN port (i.e., port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the remote NAT router is not known in advance. The chosen gateway WAN port must act as the responder.

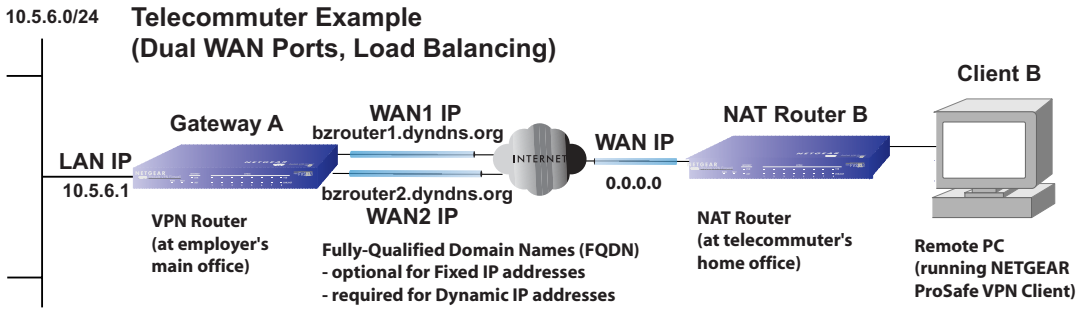

Figure 2-21: Dual gateway WAN ports (load balancing case) for VPN telecommuter

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, a fully-qualified domain name must be used. If an IP address is fixed, a fully-qualified domain name is optional.